Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Report

Security of the Business Services Online

022329 August 2024

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: August 7, 2024 **Refer to:** 022329

To: Martin O’Malley
Commissioner

From: Michelle L. Anderson Michelle L Anderson
Assistant Inspector General for Audit
as Acting Inspector General

Subject: Security of the Business Services Online

The attached final report summarizes Ernst & Young LLP’s (Ernst & Young) review of the Security of the Business Services Online.

Under a contract the Office of Audit monitored, Ernst & Young, an independent certified public accounting firm, reviewed the Business Services Online. Ernst & Young interviewed Social Security Administration staff and management and reviewed evidence the Agency provided.

Ernst & Young’s audit results contain information that, if not protected, could be used to adversely affect SSA’s information systems. In accordance with government auditing standards, we have transmitted Ernst & Young’s detailed findings and recommendations to SSA management and excluded from this summary certain sensitive information because of the potential damage if the information is misused. The omitted information neither distorts the audit results described in this report nor conceals improper or illegal practices.

If you wish to discuss the final report, please contact me or have your staff Mark Searight, Deputy Assistant Inspector General for Audit.

Attachment

TABLE OF CONTENTS

ABBREVIATIONS

BSO	Business Services Online
ERMS	Earnings Records Maintenance System
Framework	NIST Cybersecurity Framework
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
SSA	Social Security Administration

OBJECTIVE

The objective was to determine whether the Social Security Administration (SSA) has adequate controls in place that are functioning as intended to properly prevent unauthorized access and use of Business Services Online (BSO) services.

BACKGROUND

SSA's BSO is a suite of services that allows users[1] to securely exchange information with the SSA. BSO offers the following services: Report Wages to Social Security, View Name and Social Security Number Errors; Verify Social Security Number; and Internet Representative Payee Accounting Service.[2]

SSA updated controls over the BSO registration process in 2022 and 2023. Effective September 19, 2022, SSA added a step to the BSO registration process. The new step requires that users use SSA-provided activation codes. Effective March 25, 2023, SSA further updated the BSO registration process to require that users attempting to access certain services use SSA's Integrated Registration Services application for credentialing and authentication. Visitors to the employer's webpage are redirected to the Social Security Sign In page to start the authentication and registration process. To successfully register, BSO users need a separate Social Security online account or an existing Login.gov or ID.me account.

The Office of Management and Budget requires that Federal agencies implement National Institute of Standards and Technology (NIST) security controls.[3] The guidance specifies security controls for organizations and information systems that each agency can tailor based on their specific risk posture, tolerance, and appetite.

NIST Cybersecurity Framework (Framework) focuses on using business drivers to guide cyber-security activities and considering cyber-security risks as part of an organization's risk-management processes.[4] The Framework comprises three parts:

1. The Framework Core is a set of cyber-security activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational profiles.

2. Implementation Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cyber-security risk, which will help prioritize and achieve cyber-security objectives.

[1] Organizations, businesses, individuals, employers, attorneys, non-attorneys representing Social Security claimants, and third parties are collectively referred to as "users."

[2] SSA, *Business Service Online (BSO)*, ssa.gov (date last visited June 17, 2024).

[3] Office of Management and Budget, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, *M-19-17* (2019).

[4] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1, p. v (April 2018).

3. Framework Profiles help an organization align and prioritize its cyber-security activities with its business/mission requirements, risk tolerances, and resources. The Framework Profiles are divided into five functions: Identify, Protect, Detect, Respond, and Recover.[5]

SSA management is responsible for defining the policies, procedures, and processes that support the implementation of SSA's Information Security Programs, including for the Earnings Records Maintenance System (ERMS)-C environment.[6]

SCOPE AND METHODOLOGY

Ernst & Young conducted this performance audit in accordance with generally accepted government auditing standards.[7] Ernst & Young evaluated BSO in accordance with specified areas outlined in our Statement of Work's Planned Scope and Methodology.[8] These specified areas were mapped to the Framework:

- Identify
  - Governance: Determine whether the system's roles and responsibilities have been adequately defined.
  - Business Environment: Determine whether interface, business process controls, and data controls related to the business have been defined.
  - Risk Management: Determine whether management has implemented risk management controls over their cloud service providers.
- Protect
  - Identity Management and Access Controls: Determine whether the system has implemented logical access controls, role-based access, segregation of duties, and privileged account management controls.
  - Information Protection Processes and Procedures: Determine whether the system has documented and implemented the system development life-cycle, change management, and version control processes.
  - Protective Technologies: Determine whether the system (application level) has implemented a vulnerability management plan, policy, and procedures.

[5] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1, ch. 1.1, pp. 3 and 4 (April 2018).

[6] "[ERMS-C] is a major SSA application comprised of a collection of integrated sub-systems that maintain and provided for the use of major earnings files and data from individuals and employers. [The] ERMS-C project accounts for the cloud assets supporting the ERMS business processes. Its configuration contains four of the five major system groups: Annual Wage Reporting, Electronic Wage Reporting, Earnings Queries, and Earnings Corrections." SSA, *System Security Plan for Earnings Record Maintenance System - Cloud* (2023).

[7] Government Accountability Office, *Government Auditing Standards, GAO-21-368G* (April 2021).

[8] Contract Number GS-00F-290CA, Ernst & Young LLP-SSA Office of Acquisition and Grants, Task Order Number 28321323FDX030009, Attachment 1, sec. 6, pp. 65 through 72, October 31, 2022.

- Detect/Anomalies and Events: Determine whether the system has defined appropriate auditable events, security events, and implemented an appropriate monitoring process.
- Respond/Response Planning: Determine whether the system has implemented incident response plans, policies, and procedures.
- Recover/Recovery Planning: Determine whether disaster recovery processes have been documented and implemented.

See Appendix A for additional details of Ernst & Young's scope and methodology.

RESULTS OF REVIEW

We concur with Ernst and Young's findings, which concluded that BSO's controls need to be improved to ensure they are functioning as intended and additional controls are needed to properly prevent unauthorized access and use of BSO services. Ernst & Young further concluded that SSA could improve the BSO information technology system environment to ensure it fully addresses requirements outlined in its Information Security Program and related NIST Framework guidance. Specifically:

- SSA had not developed a policy for the use, functionality, and security responsibilities for all BSO services.
- SSA had not defined all roles and responsibilities for some BSO services.
- SSA had not implemented all leading security configurations and taken steps to better harden the BSO information technology system environment.

RECOMMENDATIONS

Ernst & Young provided 14 recommendations to address the identified security-related findings related to BSO. Ernst & Young transmitted the recommendations to SSA management separately.

AGENCY COMMENTS

SSA agreed with Ernst & Young's recommendations. See Appendix B for the full text of the Agency's response.

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

Scope

The Business Services Online (BSO) Supplemental In-Depth Performance Audit determined whether SSA's controls were functioning as intended to properly prevent unauthorized access and use of BSO services. The information security controls Ernst & Young selected for testing were: Security Management, Access Controls, Audit Logging & Monitoring, Change and Configuration Management, Disaster Recovery, and Incident Response. SSA defines the Earnings Records Maintenance System (ERMS)-C as ". . . a major SSA application comprised of a collection of integrated sub-systems that maintain and provided for the use of major earnings files and data from individuals and employers. [The] ERMS-C project accounts for the cloud assets supporting the ERMS business processes. Its configuration contains four of the five major system groups: Annual Wage Reporting, Electronic Wage Reporting, Earnings Queries, and Earnings Corrections."[1]

Methodology

Ernst & Young performed the procedures outlined in the Statement of Work's[2] Planned Scope and Methodology. Below are the criteria Ernst & Young used:

- Government Accountability Office, *Federal Information System Controls Audit Manual*.
- Government Accountability Office, *Government Auditing Standards*, Chapters 8 and 9.
- Office of Management and Budget Circular A-130, *Managing Federal Information as a Strategic Resource*, Appendix I, *Responsibilities for Protecting and Managing Federal Information Resources*.
- National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 5.
- NIST, Federal Information Processing Standards Publications:
    - 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004);
    - 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006); and
    - 201-3, *Personal Identity Verification of Federal Employees and Contractors* (January 2022).
- Federal Risk and Authorization Management Program *Security Assessment Framework; System Security Plan Baseline Template*; and *Continuous Monitoring Strategy & Guide*.
- SSA policies and procedures.

[1] SSA, *System Security Plan for Earnings Record Maintenance System - Cloud* (2023).

[2] Contract Number GS-00F-290CA, Ernst & Young LLP-SSA Office of Acquisition and Grants, Task Order Number 28321323FDX030009, Attachment 1, sec. 6, pp. 65 through 72, October 31, 2022.

Ernst & Young evaluated the ERMS-C implementation of SSA's information security program in accordance with specified areas mapped to the NIST Cybersecurity Framework:[3]

- Govern:
  - Roles, Responsibilities, and Authorities: Determine the roles and responsibilities for the system have been adequately defined.
  - Organizational Context: Determine whether interface, business process controls, and data controls related to the business have been defined.
- Risk Management: Determine whether management has implemented risk-management controls.
- Identify/Risk Assessments: Determine the system (application level) has implemented a vulnerability management plan, policy, and procedures.
- Protect:
  - Identity Management and Access Controls: Determine whether the system has implemented logical access controls, role-based access, segregation of duties and privileged account management controls.
  - Platform Security: Determine whether the system has documented and implemented system development life-cycle, change management, and version control processes.
- Detect/Adverse Event Analysis: Determine whether the system has defined appropriate auditable events, security events, and implemented an appropriate monitoring process.
- Respond/Incident Management: Determine whether the system has implemented incident response plans, policies, and procedures.
- Recover/Incident Recovery Plan Execution: Determine whether disaster recovery processes have been documented and implemented.

Ernst & Young considered controls outlined in the NIST cybersecurity and privacy framework profile of the NIST Special Publication (SP) 800-53, Revision 5,[4] *Security and Privacy Controls for Information Systems and Organizations*, along with the security and privacy control baselines identified in NIST for the Federal Government and adapted this guidance to assist in the control-selection process. Additionally, Ernst & Young considered the Framework's mapping to NIST SP 800-53 Revision 5 to identify additional controls.

Ernst & Young conducted walkthroughs with SSA personnel to understand the BSO information technology control environment and identified relevant policies, procedures, and processes. In

[3] NIST, *The NIST Cybersecurity Framework (CSF) 2.0* (February 2024).

[4] NIST, *Security and Privacy Controls for Information Systems and Organizations, 800-53 Revision 5* (September 2020).

addition, Ernst & Young observed controls as they occurred and inspected evidence to support the implementation of the control.

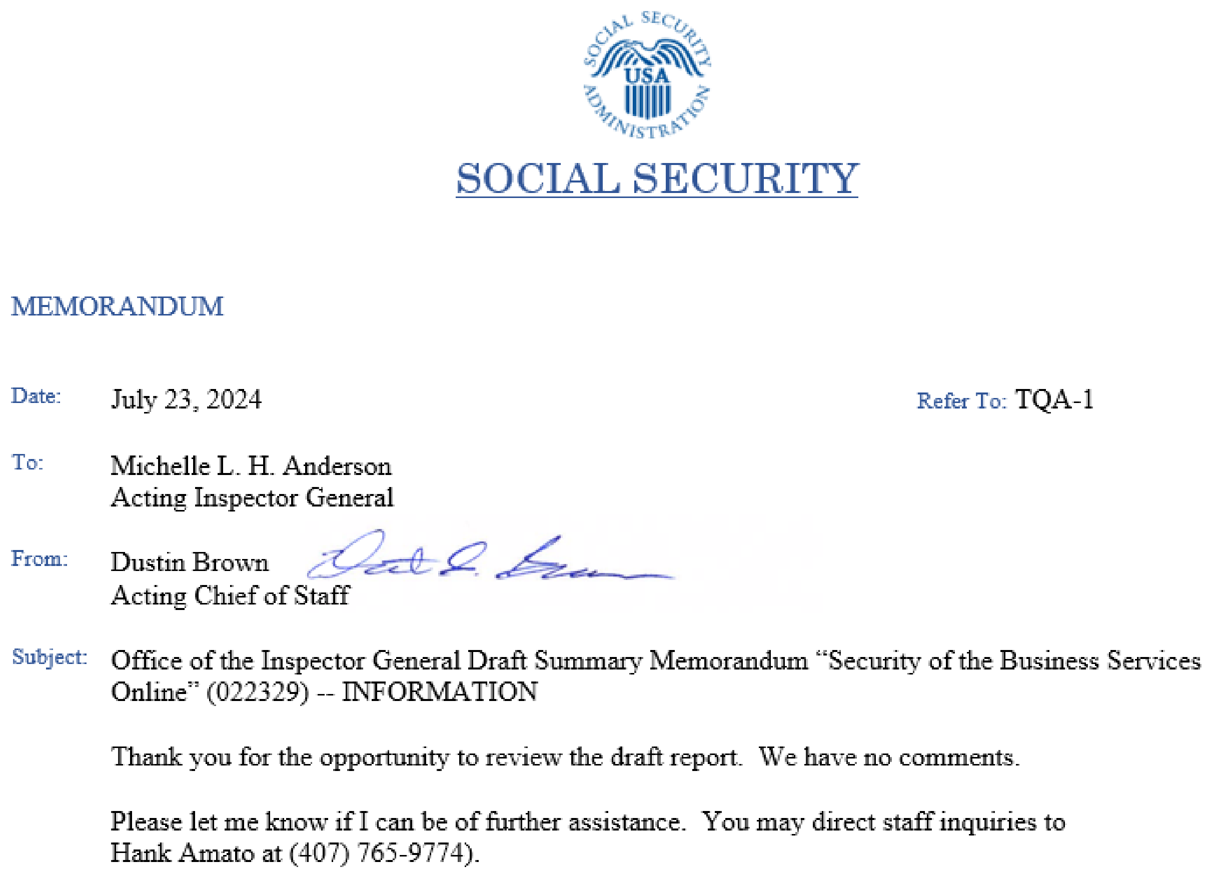
Finally, Ernst & Young performed detailed technical security controls testing with the knowledge and consent of staff in SSA's Office of Information Systems. For this testing, the team collaborated with SSA's Office of the Inspector General and designated SSA points of contact to agree on the Rules of Engagement that defined the nature, timing, and extent of the technical security work, such as diagnostic or technical security testing outside of the controls work. Ernst & Young used NIST Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment,* guidance as the foundation to define the attributes of the technical security testing.[5] This testing focused on the following domains for the ERMS-C and its subsystems to include the following:

- Application-level security vulnerabilities
    - Application review from both an authenticated and an unauthenticated user's perspective. (that is, end user, manager, administrator).
    - Interface security
    - Application security
    - Parameter injection
    - Input filtering
    - Authentication and session management
    - Sensitive data exposure
    - Authorization bypass
    - Known component weaknesses
    - Password controls
- Network architecture testing of externally facing systems (internet/intranet)
- Assessment of internal Internet Protocol addresses for exposure
- Web application firewall enablement
- Audit logging and monitoring
- Security of exposed assets through application analysis and vulnerability scanning

[5] NIST, *Technical Guide to Information Security Testing and Assessment, 800-115* (September 2008).

Ernst & Young conducted this performance audit in accordance with *Government Auditing Standards*. Those standards require that Ernst & Young plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objective. Ernst & Young believes the evidence obtained provides a reasonable basis for its findings and conclusions based on the audit objective.

Appendix B – Agency Comments



SOCIAL SECURITY

MEMORANDUM

Date:	July 23, 2024	Refer To: TQA-1
To:	Michelle L. H. Anderson Acting Inspector General	
From:	Dustin Brown Acting Chief of Staff	
Subject:	Office of the Inspector General Draft Summary Memorandum "Security of the Business Services Online" (022329) -- INFORMATION	

Thank you for the opportunity to review the draft report. We have no comments.

Please let me know if I can be of further assistance. You may direct staff inquiries to Hank Amato at (407) 765-9774).

Mission: The Social Security Office of the Inspector General (OIG) serves the public through independent oversight of SSA's programs and operations.

Report: Social Security-related scams and Social Security fraud, waste, abuse, and mismanagement, at oig.ssa.gov/report.

Connect: OIG.SSA.GOV

Visit our website to read about our audits, investigations, fraud alerts, news releases, whistleblower protection information, and more.

Follow us on social media via these external links:

X @TheSSAOIG

f OIGSSA

▶ TheSSAOIG

✉ Subscribe to email updates on our website.